

REMARKS

In paragraph 4 on pages 2 to 6 of the Official Action, claims 1, 3-7, 9, and apparently claim 12 were rejected under 35 U.S.C. 103(a) as being unpatentable over Best (U.S. Patent No. 4,465,901) in view of Rigal (U.S. Patent No. 5,881,155). Applicants respectfully traverse.

The Official Action cites Best for showing various elements of applicants' claims 1, 3-7 and 9 but recognizes that "Best does not ... specifically mention a metal shielding layer over the memory." However, in addition to failing to disclose a metal shielding layer, Best fails to disclose an electronic circuit chip having protected encryption circuitry that operates in the fashion recited in the applicants' claims. In other words, the applicants' claimed electronic circuit chip will not result merely from combining Best and Rigal.

For example, subparagraph 4(a) on page 3 of the Official Action refers to a memory and cites Best col. 4 lines 47-52 and 57-60, but the memory described in Best col. 4 lines 47-52 and 57-60 stores an enciphered program, and a crypto-microprocessor (CMP) executes the enciphered program by piecemeal deciphering of the enciphered instructions as it needs them. The applicant's "encryption procedure" should not be confused with an enciphered program. Moreover, subparagraphs 4(c) and 4(d) of the Official Action refer to Best col. 6, lines 19-21, col. 7, line 60 – col. 8, line 4 and col. 7, lines 45-47 for encryption circuitry (enciphering circuit 142 in FIG. 19 or a microprogram to encipher data output to random-access memory 151), but it is not clear that the data being enciphered is data from at least one input to the electronic chip;

instead, the data is said to be for “temporary external storage of portions of partially processed data without compromising its contents.” (Best, col. 7, lines 48-49.)

In short, Best’s crypto-microprocessor CMP “executes an enciphered program by piecemeal deciphering of enciphered instructions as it need them.” (Best, Abstract, lines 2-5; col. 3 lines 35-41; col. 4, lines 41-46.) In contrast, the electronic circuit chip of applicants’ claims is for encrypting the data from said at least one input to the electronic chip according to the encryption procedure assigned to the electronic chip, to produce encrypted data that is transmitted from at least one output from the electronic circuit chip.

Page 4 of the Official Action cites Rigal FIGS. 5 and 6 and col. 6, lines 30-37 for disclosing a metal shielding layer over the memory. However, the guard ring is not shown or described as being over a memory. It is shown and described as being a ring formed at the periphery of the protected chip 10 and on a surface of the protective chip 20. Presumably the memory containing the confidential information in Rigal would not be at the periphery of the protected chip 10, because the periphery of the protected chip would be a less secure location on the protected chip 10. Presumably the guard ring is at the periphery of the protected chip because electrical signals are conveyed between the chips in the region surrounded by the guard ring. These electrical signals are conveyed through the regions 23 and 30 in FIG. 5, which are surrounded and not covered by the guard ring 50. As shown in the cross-section of FIG. 6, most of the guard ring 50 does not even overlap the protected chip 10. Moreover, the confidential information is said to be stored in the protected chip, and the protected chip and the protective chip are said to be separated by a semiconductor resin. (Abstract). In contrast, the applicants’ claims call

for the metal layer to be part of the chip, or a layer on the chip, that contains the memory and the microprocessor programmable for encrypting data in accordance with an encryption procedure defined by information that can be stored in the memory but not read from any output of the electronic circuit chip.

Paragraph 4(g) on page 4 of the Official Action concludes:

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Best** with a metallic layer over EEPROM as taught in **Rigal**. One would have been motivated to substitute the metallic layer in **Rigal** in order to reduce tampering capability, so that the information stored in the memory cannot be read by visual inspection or probing and the information can also be resistant to interference, which enhances protection of the confidential information stored in the chip.

Applicants respectfully disagree. As discussed above, it is not seen where an integrated circuit chip in **Best** has encryption circuitry for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data; and at least one output from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry. Instead, the Official Action focuses on decryption circuitry in **Best** that decrypts an encrypted program in the memory of **Best**. In addition, as discussed above, it is not seen where the metallic guard ring of **Rigal** is over the EEPROM in the protected chip of **Rigal**. Therefore, a proper combination of

Best and Rigal would not have resulted in the applicants' invention of claims 1, 3-7, 9, or 12.

Where the prior art references fail to teach a claim limitation, there must be "concrete evidence" in the record to support an obviousness rejection. "Basic knowledge" or "common sense" is insufficient. *In re Zurko*, 258 F.3d 1379, 1385-86, 59 U.S.P.Q.2d 1693, 1697 (Fed. Cir. 2001).

Moreover, it is not seen where the cited art provides sufficient motivation for modifying a proper combination of Best and Rigal to result in the applicants' invention of claims 1, 3-7, 9, or 12. Best is directed to a microprocessor for executing computer programs which are stored in cipher to prevent software piracy. This objective is different from the applicants' objective of providing a reasonably secure electronic circuit chip that can be given a unique identity by including in the electronic circuit chip a memory for storing information defining an encryption procedure assigned to the electronic circuit chip; at least one input to the electronic circuit chip for writing, to the memory, the information defining the encryption procedure assigned to the electronic circuit chip, and for receiving data to be encrypted by the encryption procedure assigned to the electronic circuit chip; encryption circuitry for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data; and at least one output from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry.

Rigal is directed to a security device for preventing access to confidential information stored in a protected semiconductor chip. The security device comprises a second semiconductor chip with the two chips facing each other and being coupled to each other by communication terminals, and an encryption key encoded in a plurality of resistances in a semiconductor resin between the two semiconductor chips. It is not seen where Rigal would provide motivation to arrive at the applicants' claimed invention by discarding the second semiconductor chip and semiconductor resin and instead using a metal layer over the EEPROM on the protected chip to protect the confidential information in the EEPROM. Rigal appears entirely satisfactory for its intended purpose, and the proposed modification is in the opposite direction from Rigal's objective and inconsistent with Rigal's disclosure as a whole.

It is improper to attempt to establish obviousness by using the applicants' specification as a guide to combining different prior art references to achieve the results of the claimed invention. *Orthopedic Equipment Co., Inc. v. United States*, 702 F.2d 1005, 1012, 217 U.S.P.Q. 193, 199 (Fed. Cir. 1983). Hindsight reconstruction, using the applicants' specification itself as a guide, is improper because it fails to consider the subject matter of the invention "as a whole" and fails to consider the invention as of the date at which the invention was made. The critical inquiry is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *In re Dembiczak*, 175 F.3d 994, 999-1000, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999)(actual evidence and particular findings need to support the PTO's obviousness conclusion); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227

U.S.P.Q. 543, 547 (Fed. Cir. 1985) ("The invention must be viewed not with the blueprint drawn by the inventor, but in the state of the art that existed at the time."); *In re Fritch*, 972 F.2d 1260, 1266, 23 U.S.P.Q.2d 1780, 1784 (Fed. Cir. 1992)("It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious."); *Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985) (nothing of record plainly indicated that it would have been obvious to combine previously separate lithography steps into one process). See, for example, *In re Gordon et al.*, 733 F.2d 900, 902, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984) (mere fact that prior art could be modified by turning apparatus upside down does not make modification obvious unless prior art suggests desirability of modification); *Ex Parte Kaiser*, 194 U.S.P.Q. 47, 48 (PTO Bd. of Appeals 1975) (Examiner's failure to indicate anywhere in the record his reason for finding alteration of reference to be obvious militates against rejection).

Regarding applicants' claims 3 and 9, the Official Action refers to electrically alterable read-only memory in the S-boxes of Best, col. 14, lines 3-7. These S-boxes are in the address scrambler 24 of Best FIG. 8 which is used to decipher the enciphered program in Best's crypto-microprocessor.

Applicants' claim 12 defines a monolithic integrated circuit chip so it is further distinguished on this basis from the mere combination of Best and Rigal. Presumably claim 12 should be grouped with claims 2, 8, 10, and 11, as discussed below.

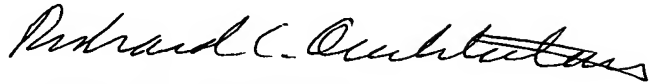
In paragraph 5 on page 7 of the Official Action, claims 2, 8, 10, and 11 were rejected under 35 U.S.C. 103(a) as being unpatentable over Best in view of Rigal and further in view of Little et al. (U.S. Patent No. 5,998,858). Applicants respectfully traverse. Little is cited for teaching a monolithic integrated circuit chip of the type having a memory that is protected by a combination of hardware and software features. (See the abstract of Little.) Although various kinds of monolithic integrated circuit chips are well known, the applicants' elegant solution of using a metal layer of a monolithic integrated circuit for a reasonable degree of protection is considerably different in a practical sense from systems of multiple chips as in Best and Rigal. Little itself describes a number of complex hardware mechanisms to prevent unauthorized accessing of the secure memory. Therefore, it is not seen how Little would have provided the required motivation to modify a proper combination of Best and Rigal to arrive at the substantially reduced complexity of the applicants' claimed invention:

Claims 10, 11, and 12 further distinguish the references by explicitly reciting that the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip. In other words, these new claims define a re-programmable tamper-resistant circuit chip that does not require any special encapsulation of the chip in or to make it tamper resistant. The complexity of the cited references themselves evidence a long felt but unsolved need to provide such an identity chip that does not require any special encapsulation of the chip in order to make it tamper resistant.

Serial No. 10/058,651
Reply to Office Action of May 6, 2004

In view of the above, reconsideration is respectfully requested, and early allowance is earnestly solicited.

Respectfully submitted,



Richard C. Auchterlonie
Reg. No. 30,607
Attorney for Assignee
NOVAK DRUCE LLP
1615 L Street, NW, Suite 850
Washington, DC 20036
713-751-0655

Date: 28 July 2004